Docket No.: 22040-00038-US1
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Makoto Izawa et al.

Application No.: 10/710,987 Confirmation No.: 4986

Filed: August 16, 2004 Art Unit: N/A

For: CENTRAL ENCRYPTION MANAGEMENT SYSTEM Examiner: Not Yet Assigned

CLAIM FOR PRIORITY AND SUBMISSION OF DOCUMENTS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant hereby claims priority under 35 U.S.C. 119 based on the following prior foreign application filed in the following foreign country on the date indicated:

Country	Application No.	Date
Japan	2002-134681	May 9, 2002

In support of this claim, a certified copy of the said original foreign application is filed herewith.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 22-0185, under Order No. 22040-00038-US1 from which the undersigned is authorized to draw.

Dated: August 17, 2004
23552_1

Respectfully submitted,

By Larry J. Hume
Larry J. Hume
Registration No.: 44,163
CONNOLLY BOVE LODGE & HUTZ LLP
1990 M Street, N.W., Suite 800
Washington, DC 20036-3425
(202) 331-7111
(202) 293-6229 (Fax)
Attorney for Applicant

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年　５月　９日

出願番号
Application Number: 特願２００２－１３４６８１

[ST. 10/C]: [ＪＰ２００２－１３４６８１]

願人
Applicant(s): 新潟精密株式会社
株式会社マイクロ総合研究所

CERTIFIED COPY OF PRIORITY DOCUMENT

２００４年　７月　５日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

【書類名】　特許願

【整理番号】　14NS1431

【提出日】　平成14年 5月 9日

【あて先】　特許庁長官殿

【国際特許分類】　G09C　1/00

【発明者】

【住所又は居所】　東京都品川区南品川２丁目２番５号　株式会社マイクロ総合研究所内

【氏名】　井澤　誠

【発明者】

【住所又は居所】　東京都品川区南品川２丁目２番５号　株式会社マイクロ総合研究所内

【氏名】　成田　宏光

【発明者】

【住所又は居所】　埼玉県上尾市緑丘４丁目７番１７号

【氏名】　岡本　明

【特許出願人】

【識別番号】　591220850

【氏名又は名称】　新潟精密株式会社

【特許出願人】

【住所又は居所】　東京都品川区南品川２丁目２番５号

【氏名又は名称】　株式会社マイクロ総合研究所

【代理人】

【識別番号】　100105784

【弁理士】

【氏名又は名称】　橘　和之

【電話番号】　049-249-5122

【手数料の表示】

【予納台帳番号】　070162

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0006161

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　暗号化の一元集中管理システム

【特許請求の範囲】

【請求項１】　暗号通信を行う複数の通信端末と、

上記複数の通信端末の間に接続され、暗号処理機能を有する通信端末との間で暗号化によるセキュリティを終端するためにデータの暗号化処理および復号化処理を行う暗号／復号手段を備えた暗号装置と、

上記暗号通信を行うのに必要な種々の情報の設定を、ネットワークを介して遠隔から上記通信端末および上記暗号装置に対して行うマネージャ端末とを備え、

上記複数の通信端末、上記マネージャ端末および上記暗号装置を有線または無線のネットワークにより接続して構成したことを特徴とする暗号化の一元集中管理システム。

【請求項２】　上記暗号／復号手段は、上記暗号処理機能が導入された通信端末との間では暗号化されたデータの通信を行うとともに、上記暗号処理機能が導入されていない通信端末との間では暗号化されていないデータの通信を行うために上記暗号化処理および上記復号化処理を行うことを特徴とする請求項１に記載の暗号化の一元集中管理システム。

【請求項３】　上記暗号装置は、一のポートより入力され上記暗号／復号手段により暗号化処理または復号化処理が施されたデータを、ルーティング処理をすることなく他のポートにそのまま出力するブリッジ手段を備えたことを特徴とする請求項１に記載の暗号化の一元集中管理システム。

【請求項４】　暗号通信を行う複数の通信端末と、

上記複数の通信端末の間に接続され、一のポートより入力され物理層およびデータリンク層を介して渡されたデータに対して暗号化処理または復号化処理を行い、これにより得られたデータを、ネットワーク間のルーティング制御を行うネットワーク層に渡すことなくデータリンク層および物理層を介して他のポートより出力する暗号装置と、

上記暗号通信を行うのに必要な種々の情報の設定を、ネットワークを介して遠隔から上記通信端末および上記暗号装置に対して行うマネージャ端末とを備え、

上記複数の通信端末、上記マネージャ端末および上記暗号装置を有線または無線のネットワークにより接続して構成したことを特徴とする暗号化の一元集中管理システム。

【請求項５】　上記暗号装置は、上記暗号化処理および上記復号化処理の制御に関して上記マネージャ端末から設定された情報を記憶する設定情報記憶手段を備え、

上記設定情報記憶手段に記憶されている設定情報と、上記一のポートより入力されたパケットに付加されているヘッダ情報とを照合して上記暗号化処理および上記復号化処理の制御を行うことを特徴とする請求項１または４に記載の暗号化の一元集中管理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は暗号化の一元集中管理システムに関し、特に、ネットワーク上で外部から攻撃されることによる情報の盗聴や改ざん等のリスクを低減するために情報の暗号化／復号化を行うシステムに用いて好適なものである。

【０００２】

【従来の技術】

パーソナルコンピュータ（パソコン）をスタンドアロンで用いる場合は、パソコン内部の情報が盗み出されたり、改ざんされたり、破壊されたりする危険性は少ない。しかし、パソコンをインターネット等のネットワークに接続すると、やり取りされる情報は多くのネットワークをルーティングされていくことから、その途中において盗聴や改ざん等の行われる危険性が一気に増大する。

【０００３】

この問題を解決するための仕組みの１つとして、情報の暗号化がある。すなわち、送信側のパソコンで情報を暗号化して相手に送り、受信側のパソコンでこれを復号化して利用する。このようにすれば、ネットワークの途中で情報が盗聴されたとしても、情報が暗号化されているために、情報自体が見られる可能性が少なくなる。また、改ざんのリスクも低減される。

【０００４】

【発明が解決しようとする課題】

しかしながら、暗号を利用するためには、暗号通信しようとする端末の全てに専用の暗号ソフトをインストールし、様々な設定をしなければならない。例えば、ある端末とある端末との間では暗号通信を行うが、他の端末との間では暗号通信を行わないなどといった暗号処理の有無、暗号通信を行う場合における暗号化のレベル、暗号化を行う時間帯、暗号鍵など、非常に多くの情報を個々の端末ごとに設定しなければならない。そのため、暗号を利用するためのシステムを構築するのに多大な労力を要するという問題があった。

【０００５】

本発明は、このような問題を解決するために成されたものであり、暗号を利用するために必要な各端末に対する様々な情報設定を簡単に行うことができるようにすることを目的とする。

【０００６】

【課題を解決するための手段】

本発明の暗号化の一元集中管理システムは、暗号通信を行う複数の通信端末と、上記複数の通信端末の間に接続され、暗号処理機能を有する通信端末との間で暗号化によるセキュリティを終端するためにデータの暗号化処理および復号化処理を行う暗号／復号手段を備えた暗号装置と、上記暗号通信を行うのに必要な種々の情報の設定を、ネットワークを介して遠隔から上記通信端末および上記暗号装置に対して行うマネージャ端末とを備え、上記複数の通信端末、上記マネージャ端末および上記暗号装置を有線または無線のネットワークにより接続して構成したことを特徴とする。

【０００７】

本発明の他の態様では、上記暗号／復号手段は、上記暗号処理機能が導入された通信端末との間では暗号化されたデータの通信を行うとともに、上記暗号処理機能が導入されていない通信端末との間では暗号化されていないデータの通信を行うために上記暗号化処理および上記復号化処理を行うことを特徴とする。

【０００８】

本発明のその他の態様では、上記暗号装置は、一のポートより入力され上記暗号／復号手段により暗号化処理または復号化処理が施されたデータを、ルーティング処理をすることなく他のポートにそのまま出力するブリッジ手段を備えたことを特徴とする。

【０００９】

本発明のその他の態様では、暗号通信を行う複数の通信端末と、上記複数の通信端末の間に接続され、一のポートより入力され物理層およびデータリンク層を介して渡されたデータに対して暗号化処理または復号化処理を行い、これにより得られたデータを、ネットワーク間のルーティング制御を行うネットワーク層に渡すことなくデータリンク層および物理層を介して他のポートより出力する暗号装置と、上記暗号通信を行うのに必要な種々の情報の設定を、ネットワークを介して遠隔から上記通信端末および上記暗号装置に対して行うマネージャ端末とを備え、上記複数の通信端末、上記マネージャ端末および上記暗号装置を有線または無線のネットワークにより接続して構成したことを特徴とする。

【００１０】

本発明のその他の態様では、上記暗号装置は、上記暗号化処理および上記復号化処理の制御に関して上記マネージャ端末から設定された情報を記憶する設定情報記憶手段を備え、上記設定情報記憶手段に記憶されている設定情報と、上記一のポートより入力されたパケットに付加されているヘッダ情報とを照合して上記暗号化処理および上記復号化処理の制御を行うことを特徴とする。

【００１１】

【発明の実施の形態】

以下、本発明の一実施形態を図面に基づいて説明する。

図１は、本実施形態による暗号化の一元集中管理システムの全体構成例を示す図である。

【００１２】

図１において、１は暗号装置であり、２つのポートを有し、一方のポートにはネットワークプリンタ２、ＤＢサーバ３、ネットワークターミナル４などのデバイスが接続され、他方のポートにはハブ５が接続されている。この暗号装置１は

、ネットワークプリンタ２、ＤＢサーバ３、ネットワークターミナル４などのデバイスと、ハブ５との間でデータの中継を行う。

【００１３】

ネットワークプリンタ２は、暗号ソフトを物理的にインストールできない端末である。ＤＢサーバ３は、動作安定上等の問題から余分な暗号ソフトをインストールすることが好ましくない端末である。ネットワークターミナル４は、ＯＳ（オペレーティングシステム）がなく暗号ソフトを動作させることができない端末である。したがって、これらの端末２～４には暗号ソフトはインストールされていないものとする。

【００１４】

また、ハブ５は、物理層においてデータを中継する機器であり、上述した暗号装置１の他に、無線通信用のアクセスポイント６、デスクトップパソコン７、暗号化／復号化に関する種々の情報設定を行うためのマネージャ端末１２が接続されている。この場合のハブ５は、暗号装置１と、アクセスポイント６およびデスクトップパソコン７との間で暗号通信のためのデータ中継を行う。また、マネージャ端末１２と、その他の暗号装置１、アクセスポイント６およびデスクトップパソコン７との間で各種情報設定のためのデータ中継も行う。

【００１５】

さらに、上記アクセスポイント６には、デスクトップパソコン８とラップトップパソコン９とが無線により接続されている。デスクトップパソコン７，８およびラップトップパソコン９には、データの暗号化および復号化を行うための暗号ソフトがインストール可能であり、実際に、暗号／復号処理を行うためのエージェントソフトがインストールされているものとする。暗号装置１にも、これと同様の暗号エージェントソフトがインストールされている。

【００１６】

このような構成により、暗号ソフトがインストールされていないネットワークプリンタ２、ＤＢサーバ３およびネットワークターミナル４と、暗号ソフトがインストールされているパソコン７～９（これらのデバイス２～４，７～９は何れも本発明の通信端末に相当）との間で、暗号装置１、ハブ５およびアクセスポイ

ント６を介してデータ通信が行われる。

【００１７】

その際、暗号装置１は、暗号ソフトがインストールされているパソコン７～９との間では暗号化されたデータの通信を行うとともに、暗号ソフトがインストールされていない端末２～４との間では暗号化されていないデータの通信を行うために暗号化処理および暗号の復号化処理を行う。

【００１８】

例えば、デスクトップパソコン７からネットワークプリンタ２にデータを送出してプリントアウトするときは、まずデスクトップパソコン７にインストールされている暗号ソフトを用いてデータを暗号化し、ハブ５を介して暗号装置１に供給する。次に暗号装置１は、受け取ったデータを復号化し、ネットワークプリンタ２に送出する。

【００１９】

また、例えばＤＢサーバ３にて管理されているデータをラップトップパソコン９に取り込むときは、ＤＢサーバ３は、与えられる要求に応じて該当するデータを暗号装置１に供給する。この暗号化されていないデータを受け取った暗号装置１は、そのデータを暗号化し、ハブ５およびアクセスポイント６を介してラップトップパソコン９に送信する。ラップトップパソコン９は、受け取ったデータを復号化し、所望の処理に利用する。

【００２０】

以上の説明から明らかなように、暗号装置１を用いることによって、専用の暗号ソフトをインストールできない端末２～４を有する企業内ＬＡＮ（Local Area Network）の中でも、暗号を利用することが可能となる。これにより、外部からの不正侵入や攻撃によってＬＡＮ内部の機密情報が盗まれたり改ざんされたりする危険性が少ないセキュアなネットワーク１０を構築することができる。

【００２１】

なお、暗号装置１と各端末２～４との間において暗号は利用できないが、これらを繋ぐケーブル１１は物理的に短い配線であり、この部分が外部アタックされることによって盗聴や改ざんが行われる可能性は極めて低いので、セキュリティ

上で特に問題となることはない。

【００２２】

上記のような暗号システムにおいて、暗号装置１および各パソコン７～９が備える暗号エージェントソフトに対して設定すべき種々の情報、例えば、暗号／復号処理の有無、ある端末とある端末との間ではパケットを破棄するなどといった通信の可否、暗号化のレベル、暗号化を行う時間帯、部門毎の暗号ポリシー、暗号鍵などの情報は、マネージャ端末１２からハブ５を介して暗号装置１および各パソコン７～９に必要な情報をダウンロードして設定する。

【００２３】

これにより、暗号の利用に必要な種々の情報を端末ごとに個別に設定する必要がなくなり、マネージャ端末１２から暗号システムの全体を一元的に集中して管理することができる。したがって、各端末に対する様々な情報設定を簡単に行うことができ、暗号システムの構築およびその後のメンテナンスにかかる労力を大幅に削減することができる。

【００２４】

従来、プリンタやファクシミリなど物理的に暗号ソフトをインストールできない端末や、プリントサーバやデータベースサーバなど余分なソフトをインストールすることが好ましくない端末、ＯＳがなく単なるネットワークターミナルとして機能する端末などを備えた企業内ＬＡＮの中では、暗号ソフトを実質的にインストールできないため、暗号を利用することは難しかった。

【００２５】

そのため、従来の暗号システムは、インターネットに接続された端末どうしがやり取りする情報を途中のインターネット上において暗号化するものであった。この場合、暗号通信する端末はインターネット上に多数散在しているため、これら多数の端末について暗号化の一元集中管理をすることは非常に困難であった。これに対して、本実施形態によれば、企業内ＬＡＮの中で暗号を利用することができるようにしているので、そのＬＡＮ内で終端された暗号化を一元的に管理することが可能となる。

【００２６】

図２は、本実施形態による暗号化の一元集中管理システムの他の構成例を示す図である。なお、この図２において、図１に示した構成要素と同一の機能を有する構成要素には同一の符号を付している。図２において、暗号装置１は、一方のポートにインターネット２０が接続され、他方のポートにハブ５が接続されている。インターネット２０の先には、図１に示したネットワークプリンタ２、ＤＢサーバ３、ネットワークターミナル４などのように暗号ソフトをインストールできない端末、あるいは、パソコン７～９のように暗号ソフトがインストールされた端末が複数台接続されている。

【００２７】

図１に示した例では、１台の暗号装置１に対して１台のデバイスが接続されており、１台のデバイスに関する暗号／復号処理を１台の暗号装置１が専用で行っていた。すなわち、図１に示す暗号装置１は、暗号ソフトがインストールされたパソコン７～９と、暗号ソフトがインストールされていない１台のデバイスとの間に接続され、暗号ソフトがインストールされたパソコン７～９との間で暗号化によるセキュリティを終端していた。

【００２８】

これに対して、図２に示す例では、暗号装置１は、暗号ソフトがインストールされたパソコン７～９と、インターネット２０に接続された複数台のデバイスとの間に接続されている。このように、暗号装置１は、複数台のデバイスに対して暗号化によるセキュリティを終端することも可能である。この場合、暗号装置１は、接続されているデバイスの数だけデータパスを有し、それぞれのデバイス毎に異なる暗号鍵で暗号／復号処理を行う。

【００２９】

上記複数台のデバイスは、暗号ソフトがインストールされていても良いし、インストールされていなくても良い。暗号ソフトがインストールされている場合には、セキュアネットワーク１０の外部にあるインターネット２０上でも暗号を利用することができる。なお、上記複数台のデバイスは、インターネット２０を介して接続されている必要は必ずしもなく、暗号装置１に直接接続しても良い。この場合、暗号装置１は２つ以上のポートを有することになる。

【００３０】

図３は、本実施形態による暗号化の一元集中管理システムの更に別の構成例を示す図である。なお、この図３において、図１に示した構成要素と同一の機能を有する構成要素には同一の符号を付している。図３に示す例も図２の例と同様に、１台の暗号装置１が複数台のデバイスに対して暗号化によるセキュリティを終端する例である。

【００３１】

図３に示す例では、セキュアネットワーク１０の内部は、３台のパソコン７～９が全てアクセスポイント6_{-1}に無線ＬＡＮにて接続されている。アクセスポイント6_{-1}は、暗号装置１を介してインターネット２０に接続されている。また、複数のアクセスポイント6_{-1}，6_{-2}を備え、１台のアクセスポイント6_{-1}でカバーしきれない通信範囲を他のアクセスポイント6_{-2}がカバーすることにより、比較的広域な無線ＬＡＮ環境を提供している。暗号装置１は、アクセスポイント6_{-1}，6_{-2}毎に個別に接続されている。

【００３２】

このように構成された暗号システムにおいて、例えば一方のアクセスポイント6_{-1}に接続されているラップトップパソコン９がその通信可能範囲を超えて移動したときには、他方のアクセスポイント6_{-2}に切り替えて通信を継続するローミングを行うことができる。しかも、上述したように、暗号通信を行うパスの設定をマネージャ端末１２により一元管理しているので、複数のアクセスポイント6_{-1}，6_{-2}間でローミングを行っても、暗号通信を継続して行うことができる。

【００３３】

また、この図３に示す例においてマネージャ端末１２は、インターネット２０に接続されている。この場合のマネージャ端末１２は、暗号エージェントソフトに対して設定すべき種々の情報を、インターネット２０を介して暗号装置１および各パソコン７～９にダウンロードして設定する。

【００３４】

なお、上記図１～図３においては、１つのセキュアネットワーク１０とその中の暗号化を一元管理する１つのマネージャ端末１２とを備える例について説明し

ている。これに対し、複数のセキュアネットワーク１０とその中の暗号化をそれぞれ一元管理する複数のマネージャ端末１２とを備え、各マネージャ端末１２がインターネット２０等を介して互いにデータ通信をして暗号化／復号化に関する種々の情報を適宜設定するようにすることにより、複数のセキュアネットワーク１０をまとめて全体として１つの暗号システムを構築することも可能である。

【００３５】

図４は、図１に示した暗号システムにおいて、暗号装置１およびこれに直接および間接的に接続されるＤＢサーバ３およびラップトップパソコン９におけるプロトコルの階層構造を示す図である。図４に示す例では、ＤＢサーバ３には暗号ソフトがインストールされておらず（ＩＰ－Ｓｅｃがない）、ラップトップパソコン９には暗号ソフトがインストールされている（ＩＰ－Ｓｅｃを有する）。このＤＢサーバ３およびラップトップパソコン９の間に、本実施形態の暗号装置１が接続されている。ここでは、ＤＢサーバ３にて保存されているデータを暗号装置１に送り、ここでデータを暗号化してパソコン９に送るような利用形態を想定している。

【００３６】

図４に示すように、ＤＢサーバ３およびパソコン９はそれぞれ１つのポート３１，３２を有し、その中継機となる暗号装置１は２つのポート３３，３４を有している。暗号装置１の各ポート３３，３４に対して物理層およびＭＡＣ層（データリンク層）が個別に設けられ、各ポート３３，３４に共通なものとしてＩＰ－Ｓｅｃ（暗号／復号処理機能）、ＩＰ層（ネットワーク層）およびＴＣＰ／ＵＤＰ層（トランスポート層）が設けられている。

【００３７】

層が深くなるほどユーザからは遠くなり、逆に層が浅くなるほどユーザに近くなる。ＤＢサーバ３およびパソコン９のＩＰ層よりも上位層には、ＴＣＰ／ＵＤＰ層およびアプリケーション層（共に図示せず）が存在し、ユーザが使用するアプリケーションと下の層との橋渡しが行われる。

【００３８】

データの送信側では、上位層から下位層に向かって各層を通過するごとにデー

タが変換されるとともに、それぞれの層間でデータ伝送を可能にするためのヘッダが付加されていく。逆に、データの受信側では、各層宛てのヘッダを参照して各層で必要なデータが抽出される。そして、抽出されたデータは上位層へ引き渡され、最終的にアプリケーション層を介してユーザに届けられる。

【００３９】

以下に、それぞれの層の機能について説明する。ＴＣＰ／ＵＤＰ層は、データを渡すべきアプリケーションの特定や、パケットの状態の管理などを行うレイヤである。データ送信側においては、上位層（アプリケーション層）から渡されたデータを相手のどのアプリケーションに渡すべきかを認識し、宛先ポート番号をデータに付加して下位層（ネットワーク層）に渡す。一方、データ受信側においては、下位層から渡されたパケットについて、通信の状態等によって抜けが生じていないかどうかを監視する。

【００４０】

ＩＰ層は、複数のネットワークにまたがった端末間のデータ転送あるいはデータ中継に関する取り決めや制御を行うためのレイヤである。通信相手となる送信側のＤＢサーバ３と受信側のパソコン９にはそれぞれ異なるＩＰアドレス①，④が割り振られており、これらを明確にすることによって、end to endによる論理的な通信経路が決定する。

【００４１】

ＭＡＣ（Media Access Control）層は、隣接機器のノード間で信頼性の高いデータ伝送を保証するためのレイヤであり、製造段階で各機器に割り当てられた物理的なＭＡＣアドレスを有する。データ送信側においては、ＩＰ層で通信相手のＩＰアドレスが明確になると、その下位に位置するＭＡＣ層において、確立された相手のＩＰアドレスをもとに、経由する次の機器（物理的に接続されている隣接ノード）の宛先を決定する。一方、データ受信側においては、ＭＡＣアドレスをもとに自分宛のパケットであることを認識した後、その上位層のＩＰ層でＩＰアドレスを解析し、そのパケットを他の機器に対して更にルーティングするか自分に取り込むかを判断する。

【００４２】

物理層は、上位層から渡されたデータを電気信号や光信号に変換し、同軸ケーブルや光ファイバケーブル等の伝送媒体を介して実際のデータ伝送を行ったり、伝送媒体から送られてきた電気信号や光信号を上位層で認識可能なデータに変換し、それを上位層に渡したりするためのレイヤである。物理層の上位層であるＭＡＣ層では、物理層の通信インタフェースに依存した手法に従って上述の処理を行う。

【００４３】

ＩＰ－Ｓｅｃは、データの暗号化処理および復号化処理を行う機能部である。すなわち、ＭＡＣ層から渡されたデータを取得して、当該データの暗号化処理および暗号の復号化処理を行う。

【００４４】

本実施形態の暗号装置１は、ＩＰ－Ｓｅｃにより２つのポート３３，３４間をブリッジさせているところに特徴がある。すなわち、本実施形態の暗号装置１では、ＤＢサーバ３とパソコン９との間におけるデータ転送に関してはＩＰ層およびＴＣＰ／ＵＤＰ層は用いず、ＩＰ層よりも下位層で処理を行う。具体的には、第１のポート３３より入力されたデータに対してＩＰ－Ｓｅｃで暗号化処理を行い、それにより得られたデータを、ＩＰ層にてルーティングすることなく（ＩＰ層に渡すことなく）他方のポートにそのまま渡して出力する。

【００４５】

すなわち、ＤＢサーバ３にて作成されたパケットデータは、当該ＤＢサーバ３のＭＡＣ層、物理層を通って送信され、暗号装置１の第１のポート３３より受信される。受信されたパケットデータは物理層、ＭＡＣ層を通ってＩＰ－Ｓｅｃに渡され、ここで暗号化処理が行われる。この暗号化されたパケットデータは、ＭＡＣ層および物理層を通って第２のポート３４より送信される。

【００４６】

第２のポート３４より送信されたパケットデータは、パソコン９で受信され、物理層、ＭＡＣ層を通ってＩＰ－Ｓｅｃに渡されて、暗号が復号化される。そして、復号化されたデータがＩＰ層を通って図示しないアプリケーション層に渡される。これにより、ＤＢサーバ３が暗号ソフトを備えていなくても、パソコン９

に対して暗号化されたデータを送信することが可能となる。

【００４７】

なお、暗号装置１のＩＰ層およびＴＣＰ／ＵＤＰ層は、上述したマネージャ端末１２から暗号装置１自身に暗号化／復号化に関する各種の情報を設定する際に利用される。この種の設定情報は、ＩＰ－Ｓｅｃブリッジの機能によってメモリ上に保持される。ＩＰ－Ｓｅｃは、当該メモリに保持されている設定情報と、ポート３３，３４より入力されたパケットに付加されているヘッダ情報（例えば、送信元ＩＰアドレスおよび宛先ＩＰアドレス）とを照合して、暗号／復号処理の制御などを行う。

【００４８】

このように、本実施形態の暗号装置１では、一のポートから入力されたデータをＩＰ－Ｓｅｃで暗号化／復号化し、これにより得られたデータをＩＰ層に渡すことなく、ルーティング処理をせずにそのまま他のポートに転送するようにしているので、データ通信時に暗号装置１のＩＰアドレスを不要とすることができる。すなわち、ＩＰアドレスを持たずにＩＰ層の暗号／復号処理を行うことが可能である。そのため、暗号装置１自身に対する煩雑なＩＰアドレス設定の必要をなくすことができる。

【００４９】

また、暗号装置１の両側に接続される端末は同じネットワークに属することになり、暗号装置１の入力ポートと出力ポートとでＩＰアドレスが変わることがなくなる。これにより、暗号装置１のネットワーク上における接続の有無に関わりなく、ＩＰアドレスの透過性を保つことができる。すなわち、ネットワーク上に暗号装置１を接続したり、ネットワーク上から暗号装置１を外したりする際に、当該暗号装置１に接続される端末のアドレス設定も変更する必要がない。

【００５０】

例えば、図４のようにＤＢサーバ３とパソコン９との間に暗号装置１を挿入した場合も、暗号装置１を挿入せずにＤＢサーバ３とパソコン９との間で直接通信を行う場合も、ＤＢサーバ３とパソコン９との間を流れるパケットのＩＰアドレスは、図５に示す通りのままで不変である。したがって、暗号装置１の接続の有

無によってアドレス設定を何ら変更する必要がない。

【００５１】

これにより、ネットワークシステムの導入時やメンテナンス時には、本実施形態の暗号装置１を適当な箇所にただ挿入したり、あるいはただ取り外したりするだけ良くなり、煩雑なアドレス設定は行う必要がないので、作業負荷を大幅に削減することができる。

【００５２】

さらに、本実施形態の場合、ＭＡＣアドレスについても透過性を保つことができる。図６は、ＤＢサーバ３からパソコン９にデータを送り、その間の暗号装置１でデータを暗号化する場合におけるパケットを示す図である。図６（ａ）は第１のポート３３にて受信するパケットを示し、図６（ｂ）は第２のポート３４より送信するパケットを示す。なお、ＩＰ－Ｓｅｃには、データ部のみを暗号化するトランスポートモードと、パケット全てを暗号化して更に新しいヘッダを追加するトンネルモードとがある。送信パケットに関しては、これら２つのモードについてそれぞれ示している。

【００５３】

また、図７は、本実施形態との比較のために、従来のＶＰＮルータを用いたシステムにおいて一方のパソコンから他方のパソコンにデータを送り、その間のＶＰＮルータでデータを暗号化する場合におけるパケットを示す図である。図７（ａ）はＶＰＮルータの第１のポートにて受信するパケットを示し、図７（ｂ）は第２のポートより送信するパケットを示す。この図７においても、送信パケットに関しては、２つのモードについてそれぞれ示している。

【００５４】

図６から明らかなように、本実施形態によれば、ＩＰアドレスだけでなく、ＭＡＣアドレスについても第１のポート３３と第２のポート３４とで異なることがなく、ＭＡＣアドレスの透過性を保つことができる。すなわち、本実施形態の暗号装置１は、ＩＰ－Ｓｅｃを有してデータの暗号／復号処理を行うことを除けば、一方のポートから入力されたデータを他方のポートにただ流すだけなので、データ通信時にはＭＡＣアドレスも不要とすることができる。

【００５５】

なお、以上に説明した実施形態は、本発明を実施するにあたっての具体化の一例を示したものに過ぎず、これによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその精神、またはその主要な特徴から逸脱することなく、様々な形で実施することができる。

【００５６】

【発明の効果】

本発明は上述したように、例えば暗号処理機能が導入された端末との間で暗号化によるセキュリティを終端するために暗号化処理および暗号の復号化処理を行う暗号／復号手段を備えて暗号装置を構成し、この暗号装置と、暗号通信を行う複数の通信端末と、暗号通信を行うために必要な種々の情報の設定を遠隔から通信端末および暗号装置に対して行うマネージャ端末とを接続して暗号システムを構成するようにしたので、専用の暗号ソフトをインストールできない端末を有する企業内ＬＡＮの中でも暗号を利用することができるようになり、そのＬＡＮ内で終端された暗号化をマネージャ端末において一元的に集中管理することが可能となる。これにより、暗号システムの構築およびその後のメンテナンスにかかる労力を大幅に削減することができる。

【図面の簡単な説明】

【図１】

本実施形態による暗号化の一元集中管理システムの構成例を示す図である。

【図２】

本実施形態による暗号化の一元集中管理システムの他の構成例を示す図である。

【図３】

本実施形態による暗号化の一元集中管理システムの更に別の構成例を示す図である。

【図４】

本実施形態による暗号装置およびこれに接続されるＤＢサーバおよびパソコンにおけるプロトコルの階層構造を示す図である。

【図５】

本実施形態においてネットワーク上を流れるパケットのＩＰアドレスについて説明するための図である。

【図６】

本実施形態の暗号装置を流れるパケットのＭＡＣアドレスについて説明するための図である。

【図７】

従来のＶＰＮルータを流れるパケットのＭＡＣアドレスについて説明するための図である。

【符号の説明】

１　暗号装置

２　ネットワークプリンタ

３　ＤＢサーバ

４　ネットワークターミナル

５　ハブ

６　アクセスポイント

７，８　デスクトップパソコン

９　ラップトップパソコン

１０　セキュアネットワーク

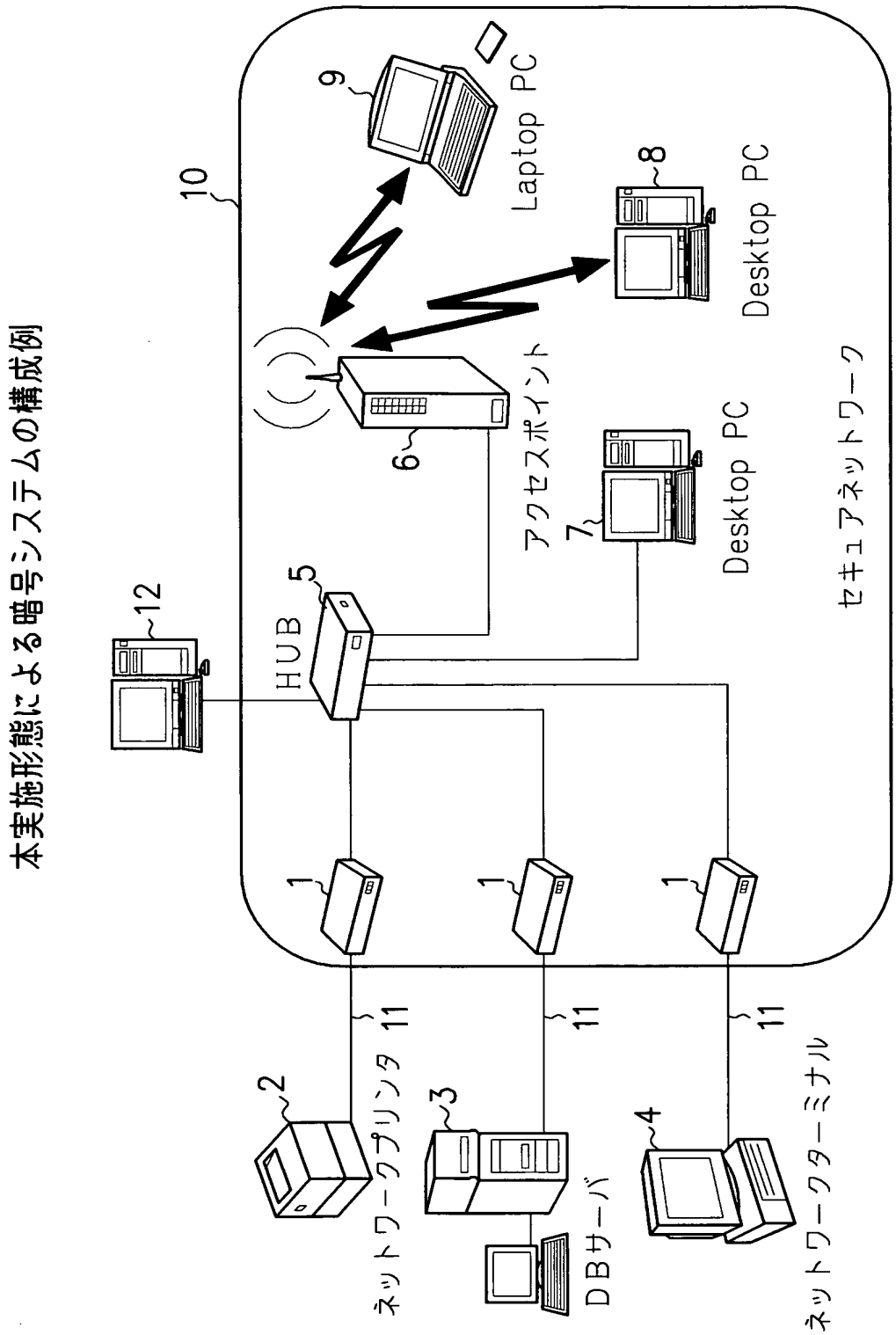
１１　ケーブル

１２　マネージャ端末

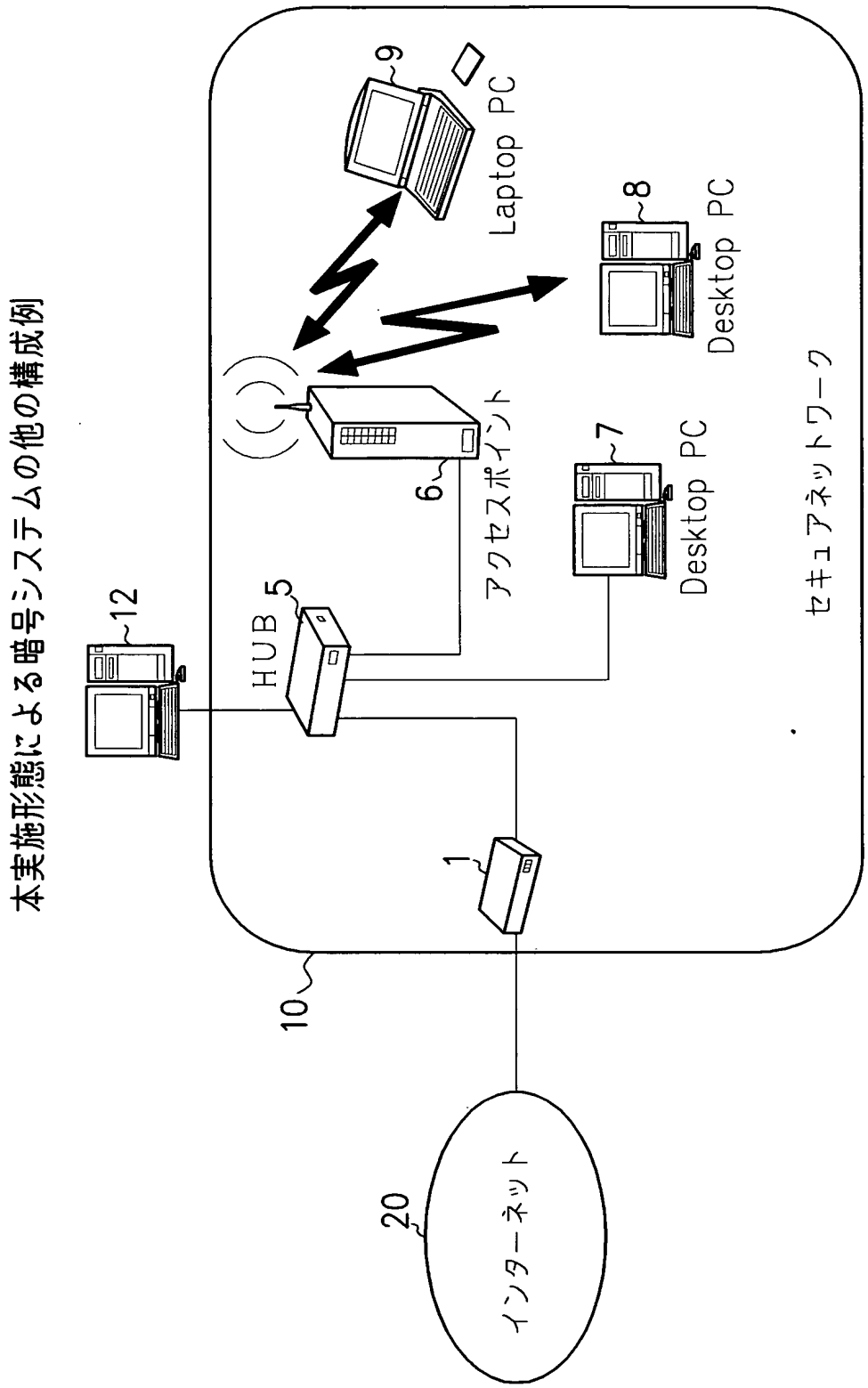
２０　インターネット

【書類名】　図面

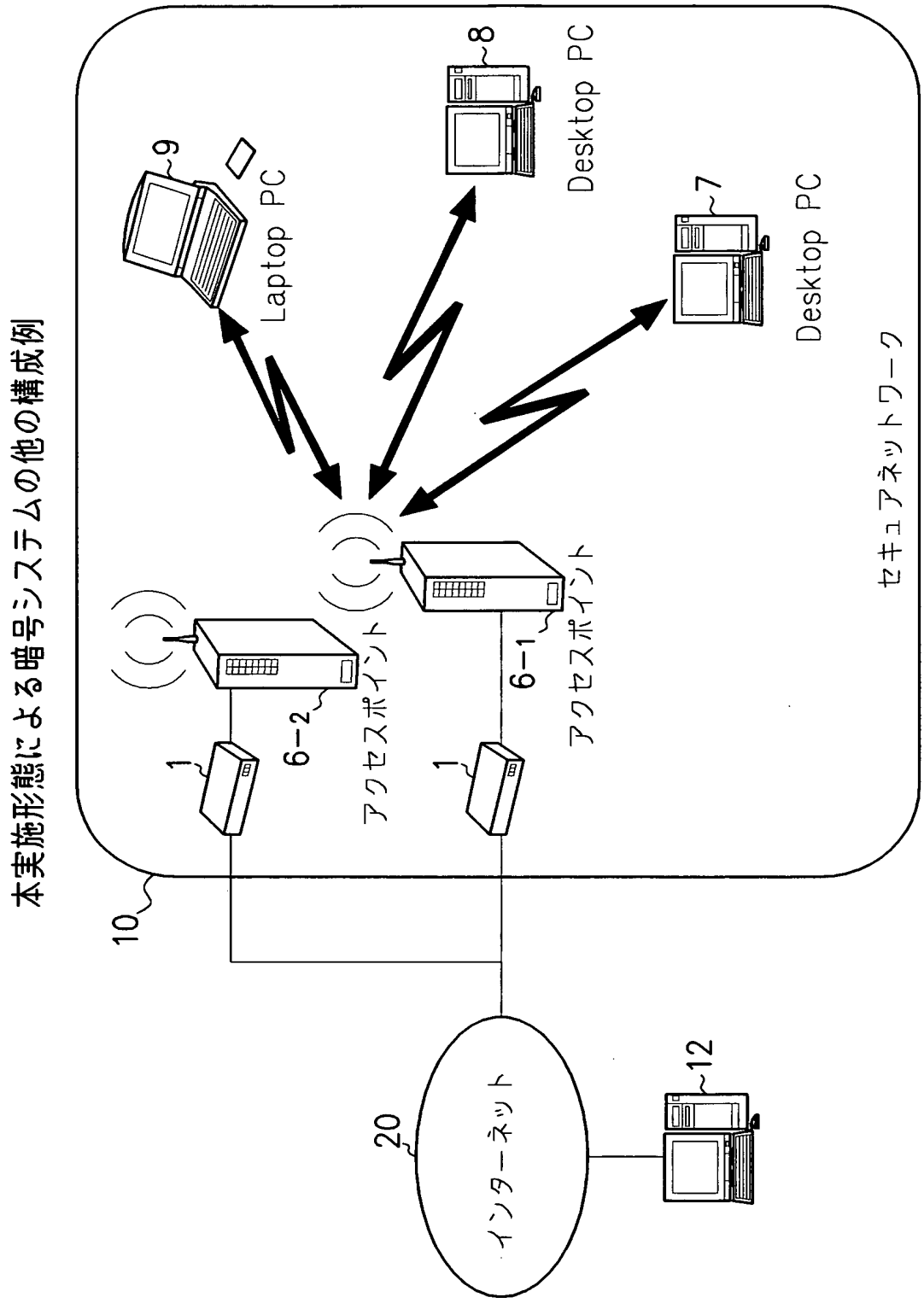
【図１】


本実施形態による暗号システムの構成例
10
9
Laptop PC
8
Desktop PC
6
アクセスポイント
7
Desktop PC
セキュアネットワーク
12
HUB
5
1
1
1
11
11
11
2
3
4
ネットワークプリンタ
DBサーバ
ネットワークターミナル

【図２】

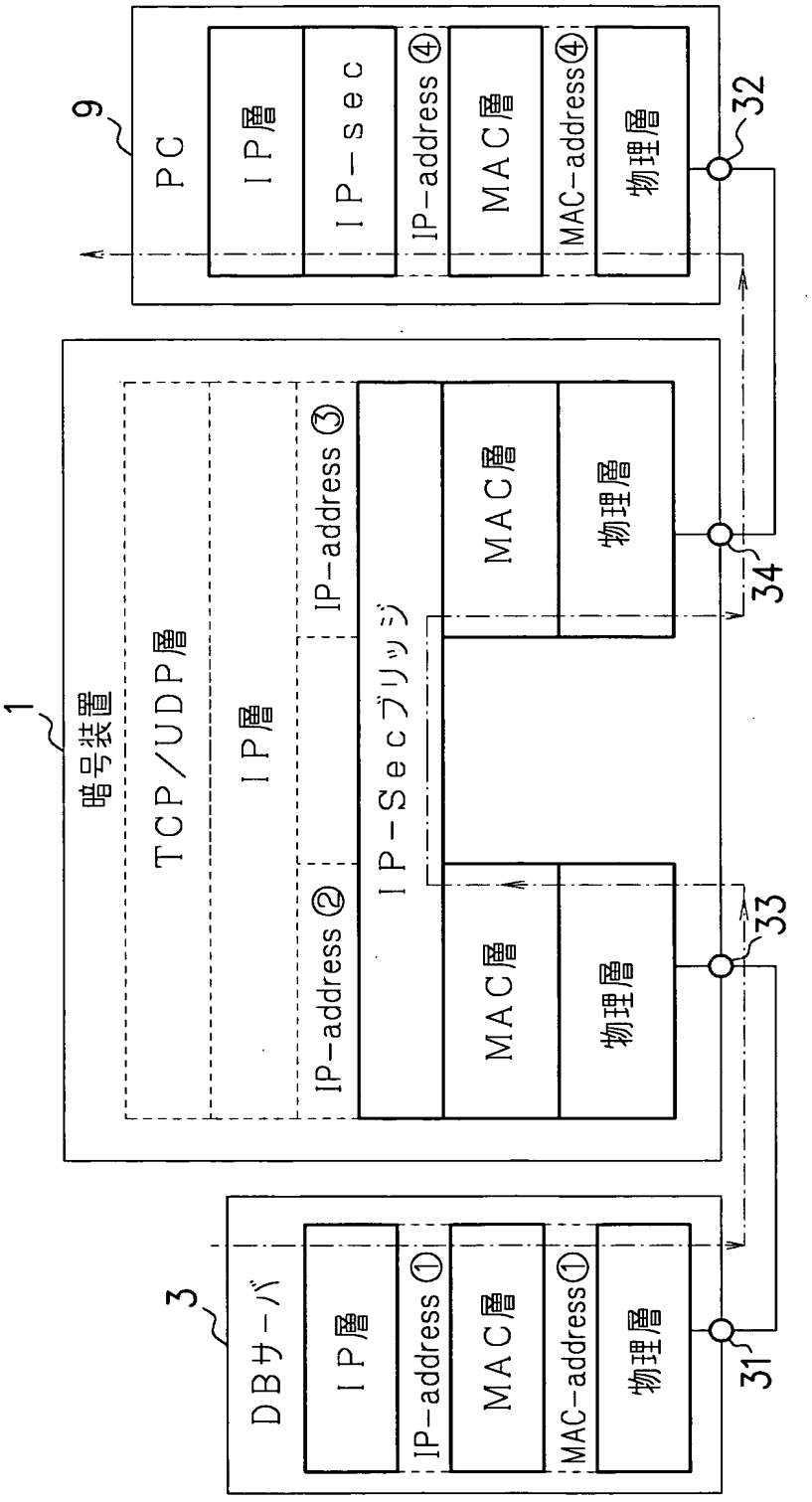

本実施形態による暗号システムの他の構成例
9
Laptop PC
8
Desktop PC
6
アクセスポイント
7
Desktop PC
セキュアネットワーク
12
HUB
5
1
10
20
インターネット

【図３】


本実施形態による暗号システムの他の構成例
セキュアネットワーク
Laptop PC
Desktop PC
Desktop PC
アクセスポイント
アクセスポイント
インターネット
9
8
7
6-1
6-2
1
1
10
20
12

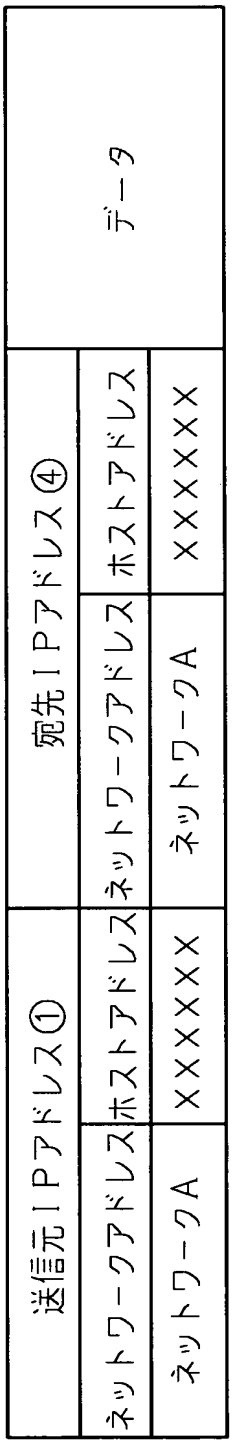
【図４】

本実施形態による暗号装置のレイヤ構造

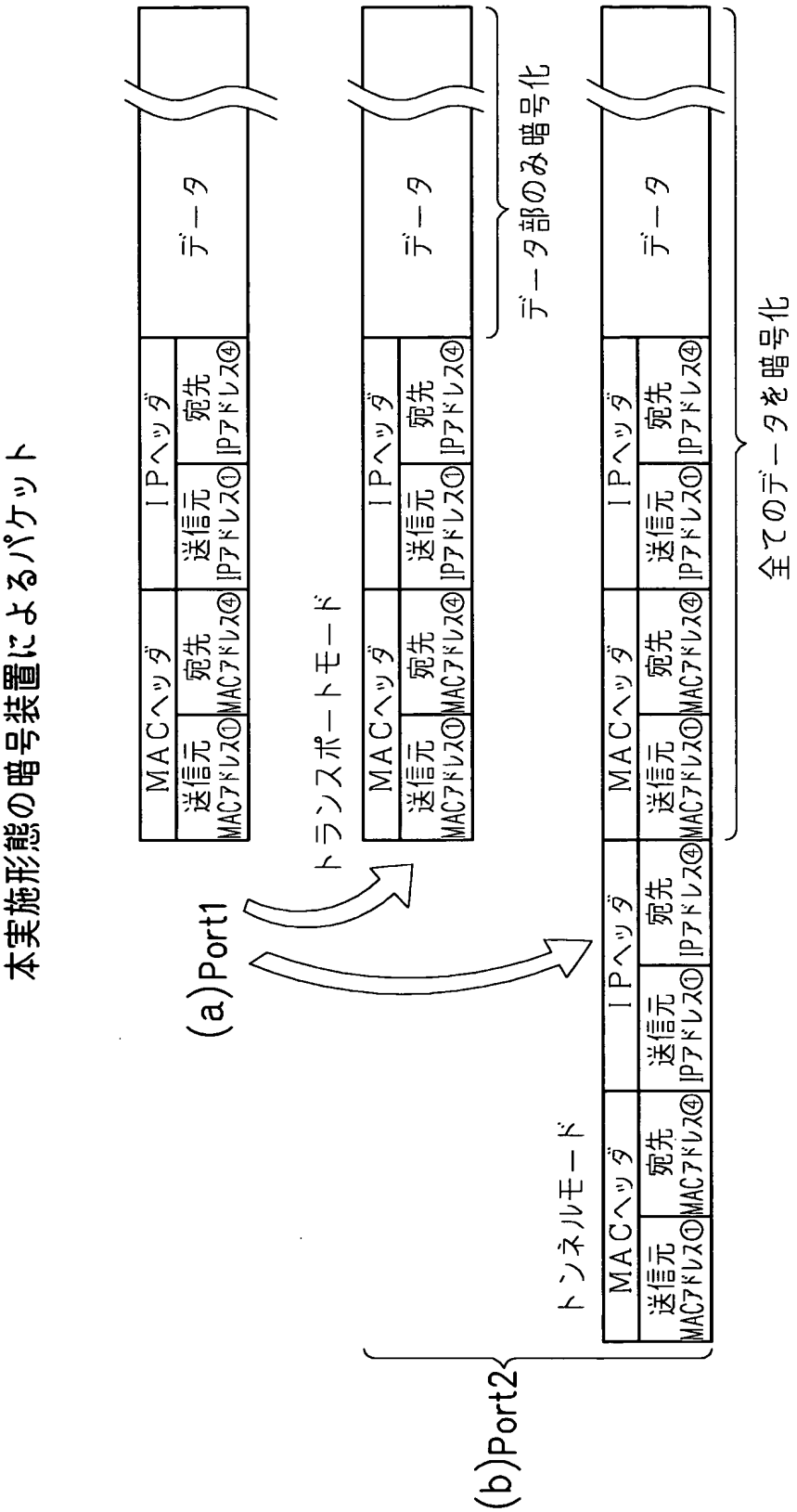


【図５】

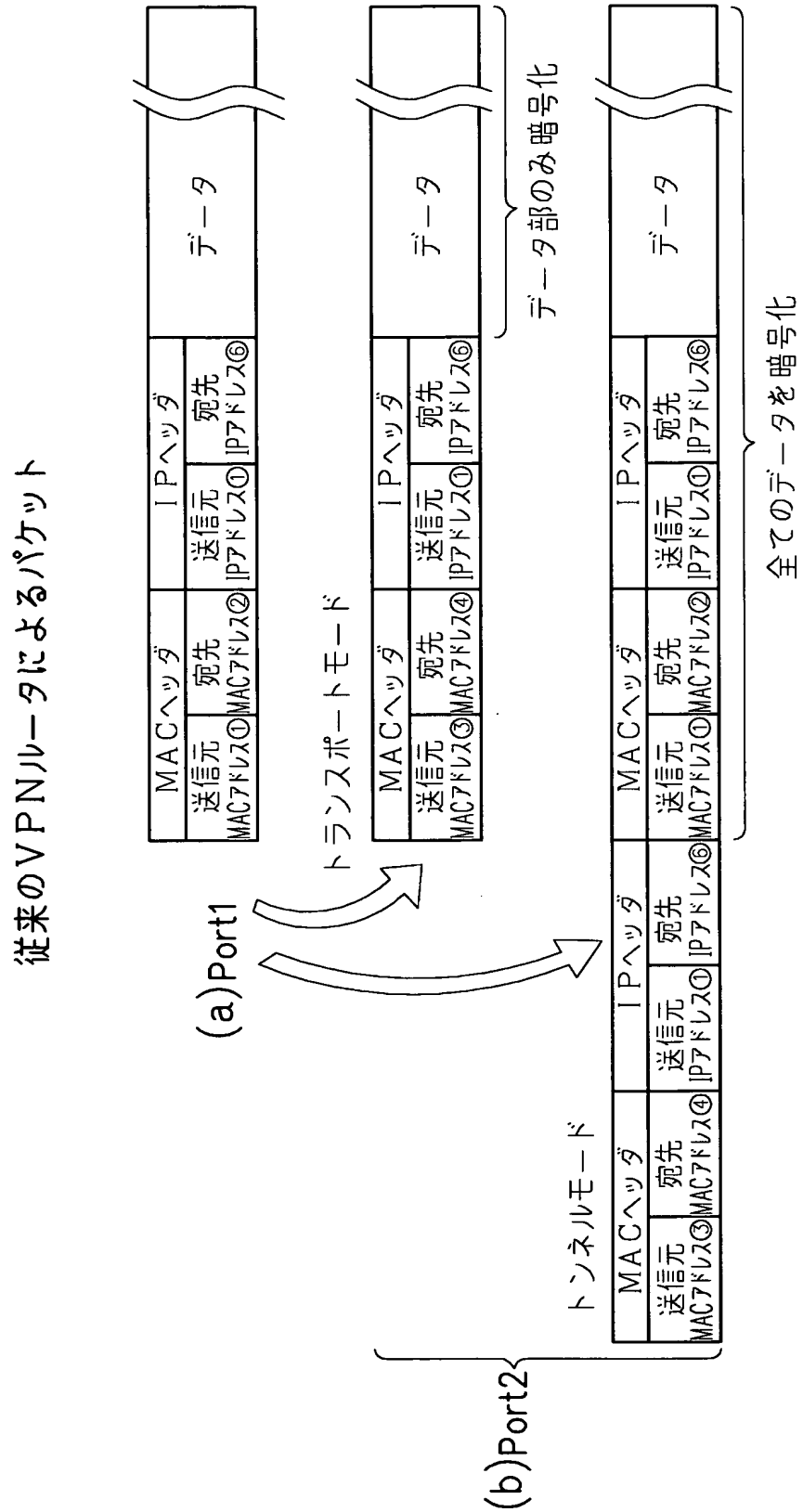
本実施形態のパケット



【図６】


本実施形態の暗号装置によるパケット
(a)Port1
トランスポートモード
データ部のみ暗号化
(b)Port2
トンネルモード
全てのデータを暗号化
MACヘッダ
IPヘッダ
データ
送信元MACアドレス①
宛先MACアドレス④
送信元IPアドレス①
宛先IPアドレス④

【図７】


従来のVPNルータによるパケット
(a)Port1
トランスポートモード
MACヘッダ
送信元MACアドレス①
宛先MACアドレス②
IPヘッダ
送信元IPアドレス①
宛先IPアドレス⑥
データ
MACヘッダ
送信元MACアドレス③
宛先MACアドレス④
IPヘッダ
送信元IPアドレス①
宛先IPアドレス⑥
データ
データ部のみ暗号化
(b)Port2
トンネルモード
MACヘッダ
送信元MACアドレス③
宛先MACアドレス④
IPヘッダ
送信元IPアドレス①
宛先IPアドレス⑥
MACヘッダ
送信元MACアドレス①
宛先MACアドレス②
IPヘッダ
送信元IPアドレス①
宛先IPアドレス⑥
データ
全てのデータを暗号化

【書類名】　　要約書

【要約】

【課題】　暗号を利用するために必要な各端末に対する様々な情報設定を簡単に行うことができるようにする。

【解決手段】　暗号処理機能が導入された端末との間で暗号化によるセキュリティを終端するために暗号化処理および暗号の復号化処理を行う暗号／復号手段を備えて暗号装置１を構成し、この暗号装置１と、暗号通信を行う複数の通信端末２～９と、暗号通信に必要な種々の情報の設定を遠隔から通信端末７～９および暗号装置１に対して行うマネージャ端末１２とを接続して暗号システムを構成することにより、専用の暗号ソフトをインストールできない端末を有する企業内ＬＡＮの中でも暗号を利用することができるようにして、そのＬＡＮ内で終端された暗号化をマネージャ端末１２において一元的に集中管理することができるようにする。

【選択図】　　図１

特願２００２－１３４６８１

出　願　人　履　歴　情　報

識別番号　　［５９１２２０８５０］

１．変更年月日　　１９９６年　５月　９日
［変更理由］　　住所変更
住　所　　新潟県上越市西城町２丁目５番１３号
氏　名　　新潟精密株式会社

特願２００２－１３４６８１

出　願　人　履　歴　情　報

識別番号　［５０１３０６９７７］

１．変更年月日　２００１年　８月　２日
［変更理由］　新規登録
住　所　東京都品川区南品川２丁目２番５号
氏　名　株式会社マイクロ総合研究所